Пример настройки TACACS + на точке доступа Aironet для проверки подлинности пользователей при входе в систему с использованием GUI

Содержание

Введение

Этот документ объясняет, как включить TACACS Плюс (TACACS +) сервисы на точке доступа Cisco Aironet (AP) для выполнения login authentication с использованием TACACS + сервер.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Знание того, как настроить основные параметры на AP Aironet
- Знание того, как настроить TACACS + сервер как сервер Cisco Secure Access Control Server (ACS)
- Знание TACACS + понятия

Для получения информации о том, как работает TACACS +, обратитесь к *TACACS*

Понимания + раздел RADIUS Настройки и TACACS + Серверы.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco Aironet aironet 1240 / точки доступа серии 1140
- ACS, который работает под управлением ПО версии 4.1
- ACS, который работает под управлением ПО версии 5.2

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Настройка

Этот раздел объясняет, как настроить AP Aironet и TACACS + сервер (ACS) для TACACS +-based login authentication.

Этот пример конфигурации использует эти параметры:

- IP-адрес ACS — 172.16.1.1/255.255.0.0
- IP-адрес AP — 172.16.1.30/255.255.0.0
- Общий секретный ключ, который используется на AP и TACACS + сервер — **Пример**

Это учетные данные пользователя, которого данный пример настраивает на ACS:

- Имя пользователя — **User1**
- **Password cisco**
- Группа — **AdminUsers**

Необходимо настроить TACACS + функции для проверки пользователей, которые пытаются соединиться с AP или через веб-интерфейс или через интерфейс командной строки (CLI). Для выполнения этой конфигурации необходимо выполнить эти задачи:

1. Настройте TACACS + сервер для login authentication.
2. Настройте AP Aironet для TACACS + аутентификация.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

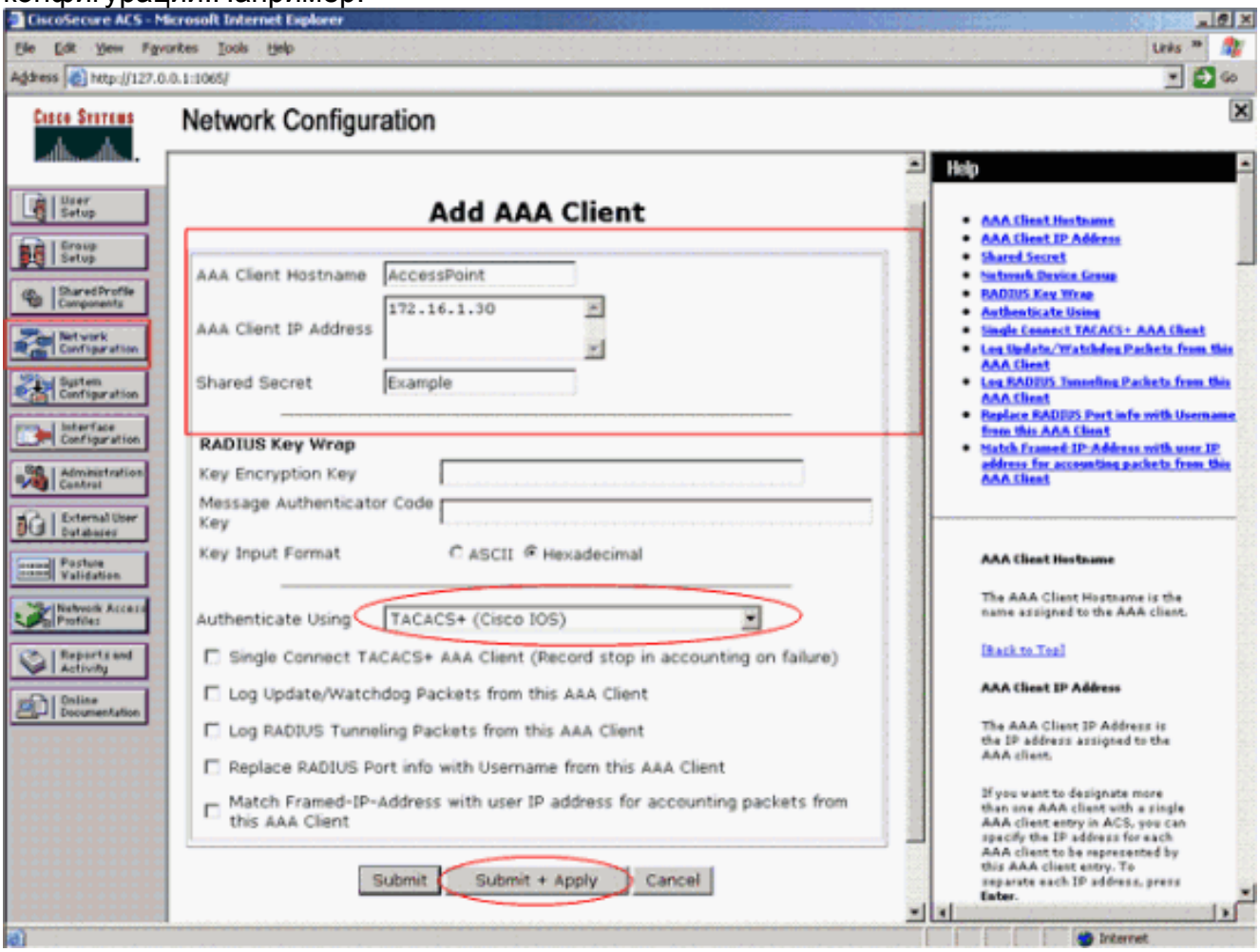
Схема сети

В настоящем документе используется следующая схема сети:

Настройте TACACS + сервер для Login Authentication - Использование ACS 4.1

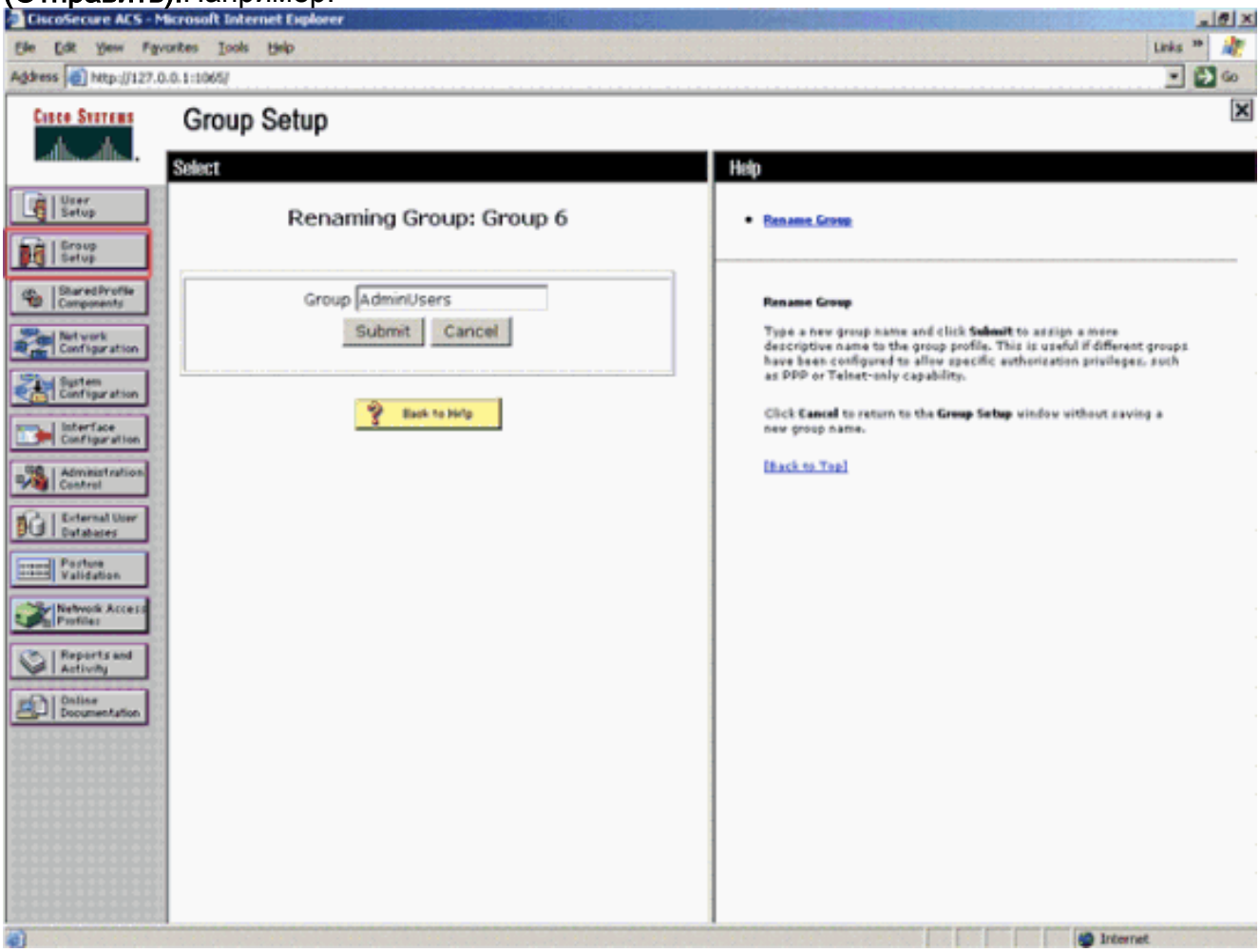
Первый шаг должен установить TACACS + демон для проверки пользователей, которые пытаются обратиться к AP. Необходимо установить ACS для TACACS + аутентификация и создать базу данных пользователей. Можно использовать любой TACACS + сервер. Данный пример использует ACS в качестве TACACS + сервер. Выполните следующие действия:

1. Выполните эти шаги для добавления AP как клиент аутентификации, авторизации и учета (AAA):От GUI ACS нажмите вкладку **Network Configuration**.**На вкладке AAA Clients (Клиенты AAA) щелкните Add Entry (Добавить запись).**В окне Add AAA Client введите имя хоста AP, IP-адрес AP и общий секретный ключ.Этот общий секретный ключ должен совпасть с общим секретным ключом, который вы настраиваете на AP.От раскрывающегося меню Используемой аутентификации выберите **TACACS + (Cisco IOS)**.Нажмите **Submit + Перезапуск** для сохранения конфигурации.Например:

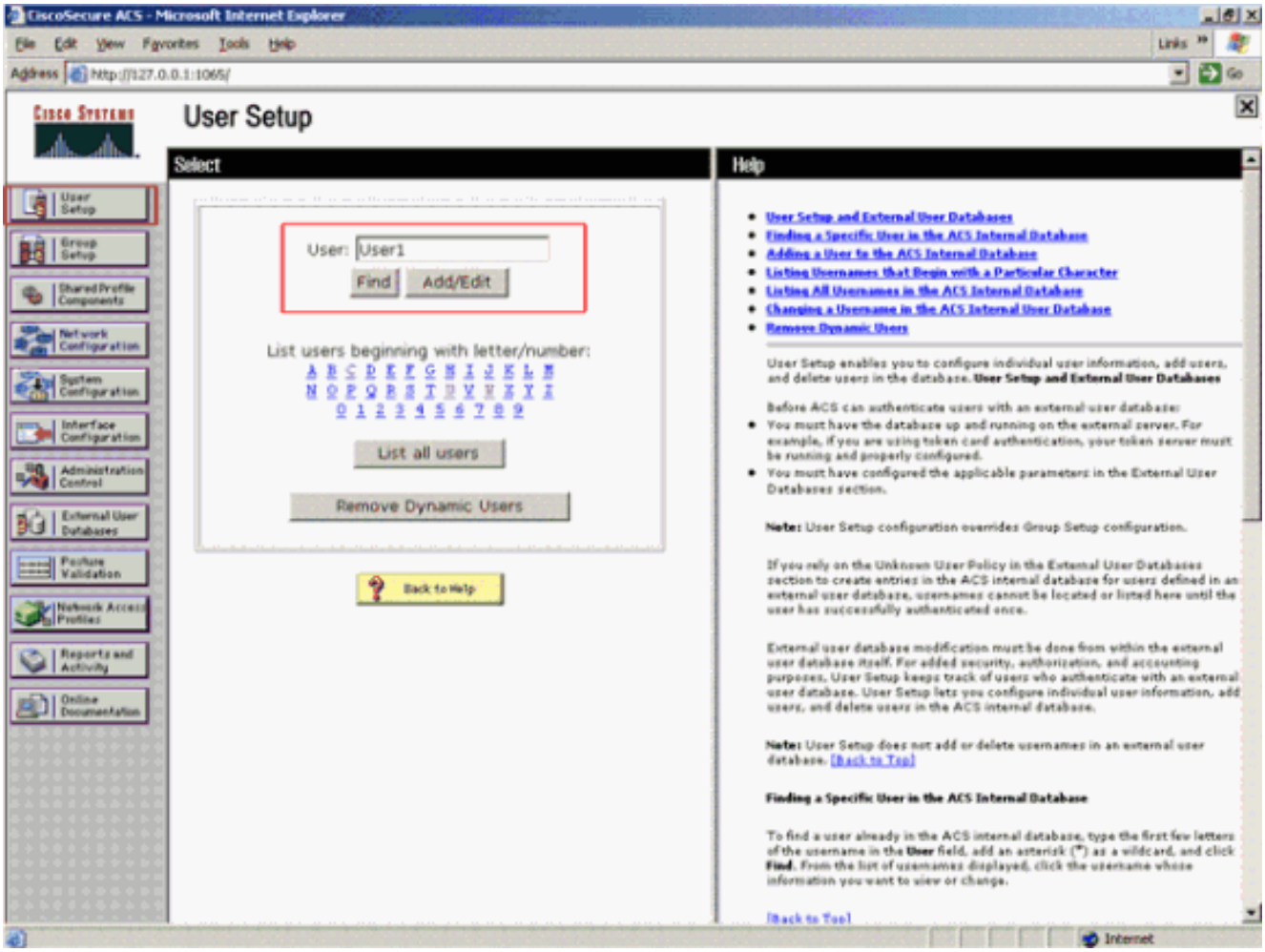


Использование данного примера:Имя хоста для клиента AAA **AccessPoint**Адрес **172.16.1.30/16** как IP-адрес клиента AAA**Пример** общего секретного ключа

2. Выполните эти шаги для создания группы, которая содержит все административное (admin) пользователи:Нажмите **Group Setup** из меню слева.Новое окно появляется.В окне Group Setup выберите группу, чтобы настроить от раскрывающегося меню и нажать **Rename Group**.Данный пример выбирает Group 6 от раскрывающегося меню и переименовывает группу AdminUsers.**Нажмите кнопку Submit (Отправить).**Например:

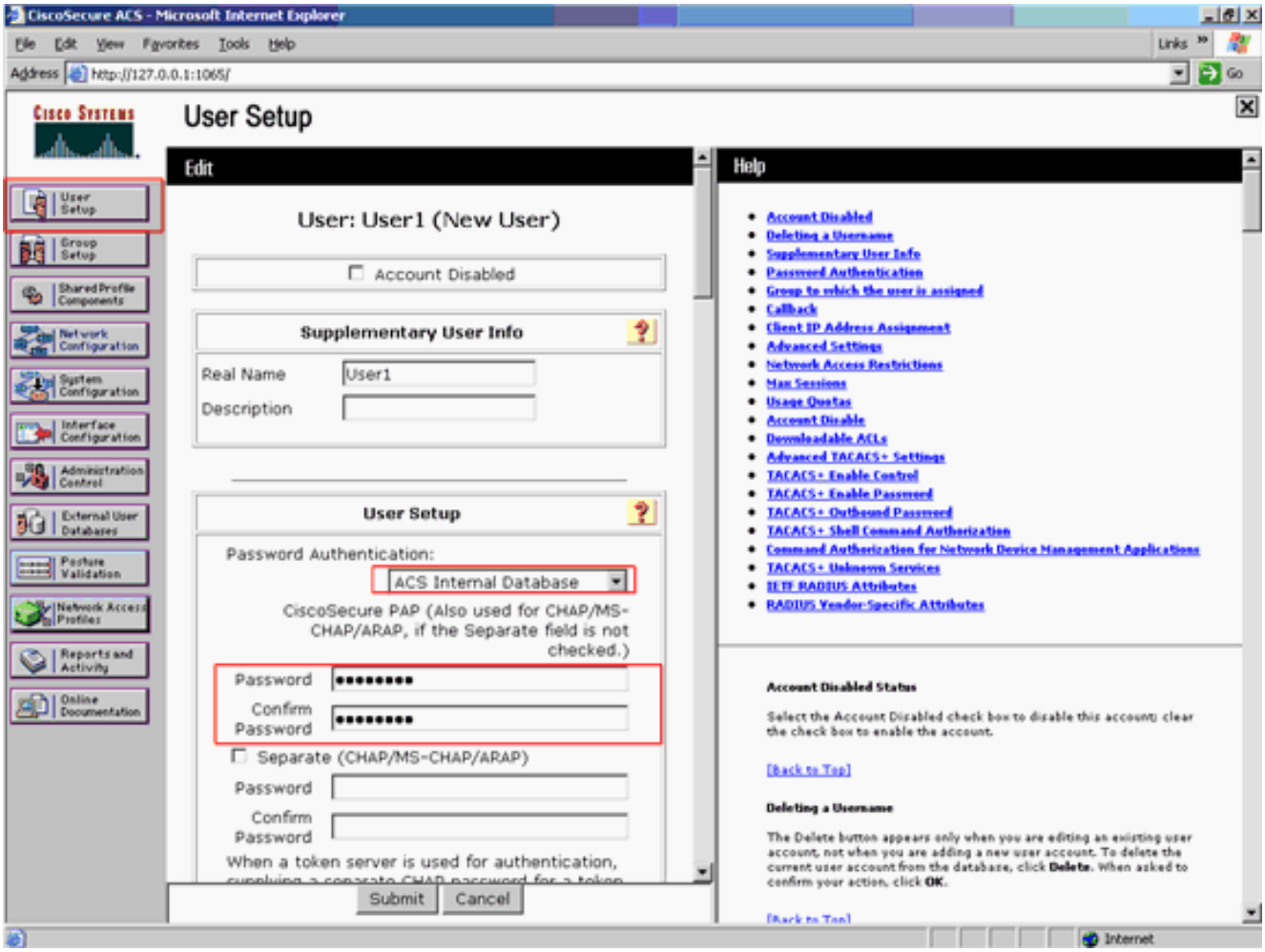


3. Выполните эти шаги для добавления пользователей к TACACS + база данных:Нажмите вкладку **User Setup**.Для создания нового пользователя введите имя пользователя в поле User и нажмите **Add/Edit**.Вот пример, который создает **User1**:

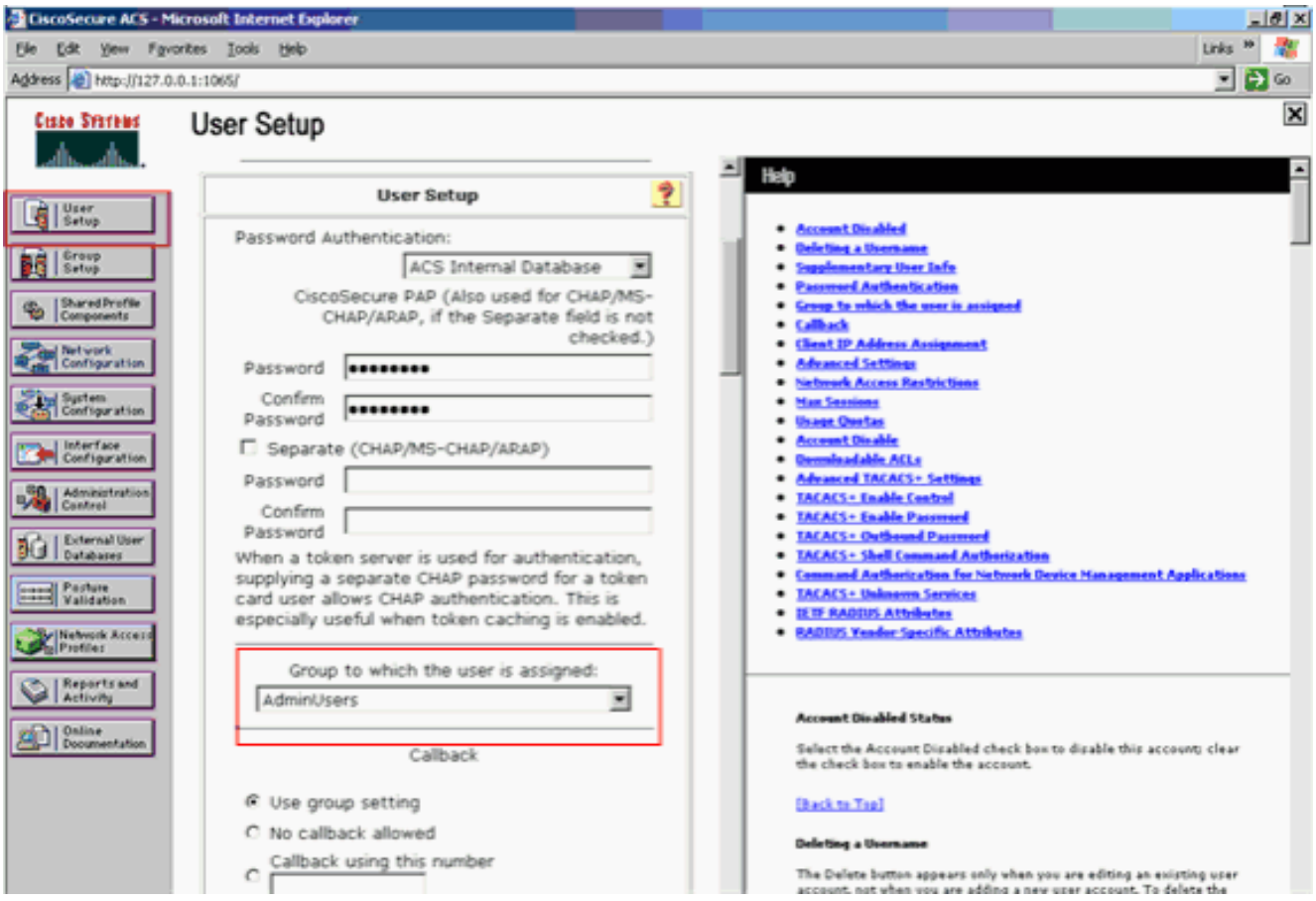


После нажатия Add/Edit Add/Edit window для этого пользователя появляется.

4. Введите учетные данные, которые являются определенными для этого пользователя и нажимают **Submit** для сохранения конфигурации.Учетные данные, которые можно ввести, включают:Дополнительные сведения о пользователеНастройки пользователяГруппа, на которую назначают пользователюНапример:



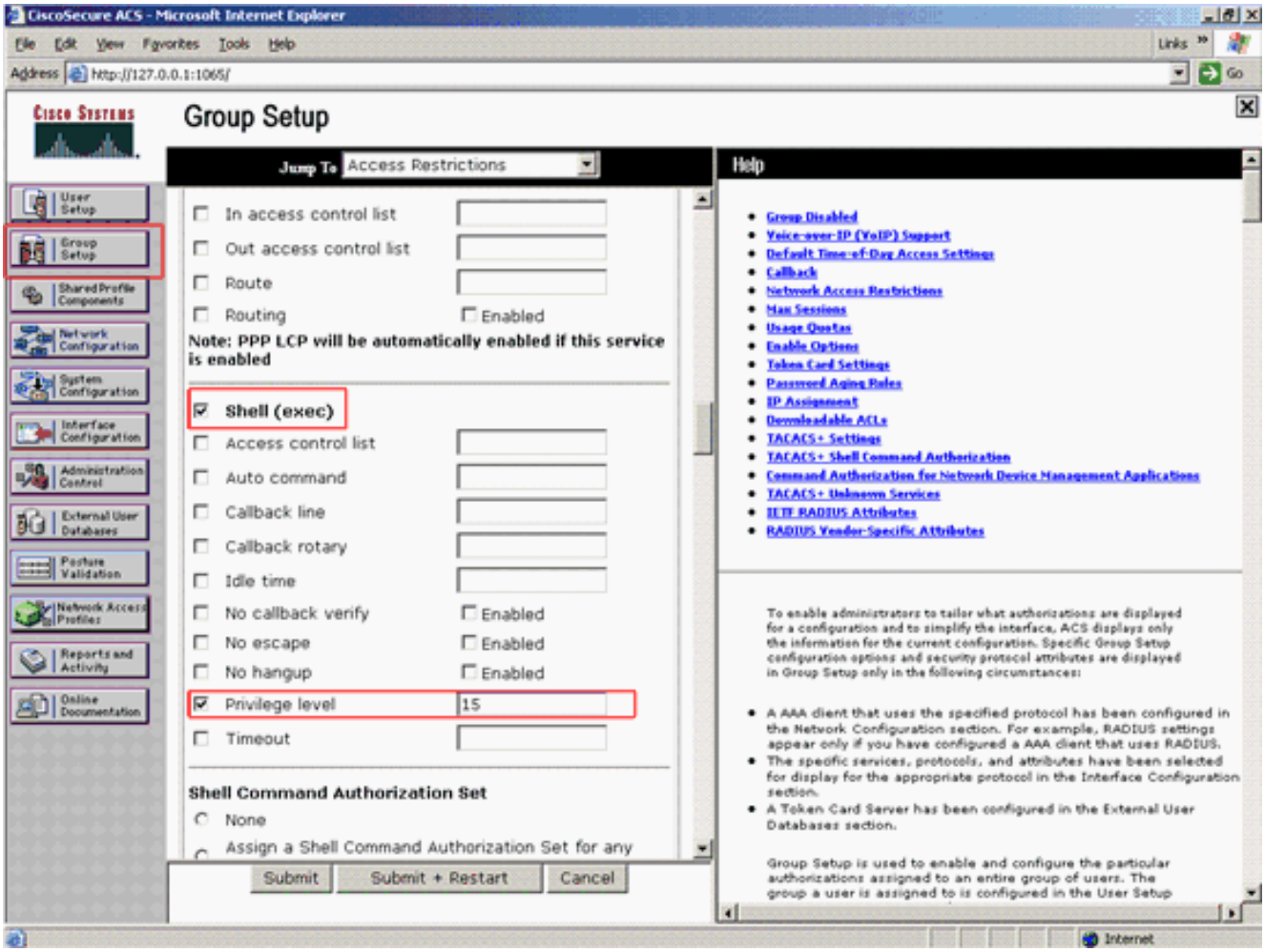
Вы видите, что данный пример добавляет пользовательский User1 к группе AdminUsers.



Примечание: Если вы не создаете определенную группу, пользователей назначают на

группу по умолчанию.

5. Выполните эти шаги для определения уровня привилегий:Нажмите вкладку **Group Setup**.Выберите группу, которую вы ранее назначили на этого пользователя, и нажмите **Edit Settings**.Данный пример использует группу AdminUsers.Под TACACS + Параметры настройки, проверьте флажок **Shell (exec)** и проверьте **флажок Privilege level**, который имеет значение 15.**Нажмите Submit + Restart.**



Примечание: Уровень привилегий 15 должен быть определен для GUI и Telnet, чтобы быть доступным как уровень 15. В противном случае, по умолчанию, пользователь может только обратиться как уровень 1. Если уровень привилегий не определен, и пользователь пытается войти в привилегированный режим на CLI (с использованием Telnet), AP отображает это сообщение об ошибках:`AccessPoint>enable % Error in authentication`

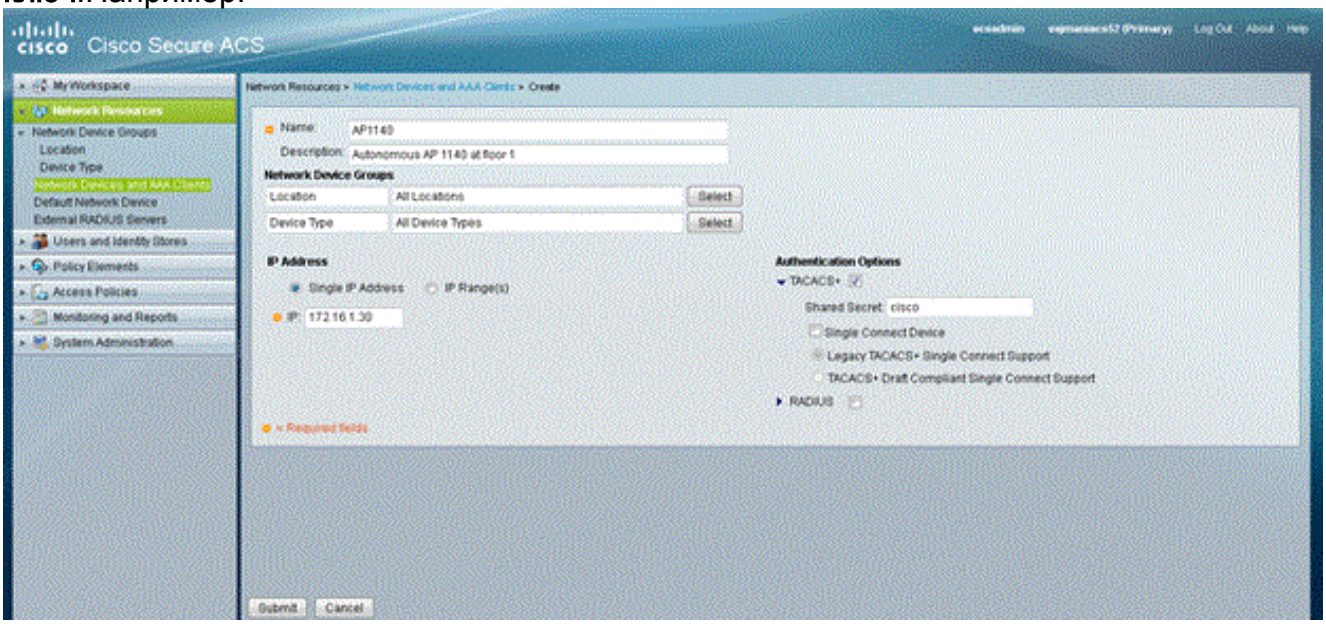
Повторите шаги 2 - 4 этой процедуры, если вы хотите добавить больше пользователей к TACACS + база данных. После того, как вы выполнили эти шаги, TACACS +, сервер готов проверить пользователей, которые пытаются войти к AP. Теперь, необходимо настроить AP для TACACS + аутентификация.

Настройте TACACS + сервер для Login Authentication - Использование ACS 5.2

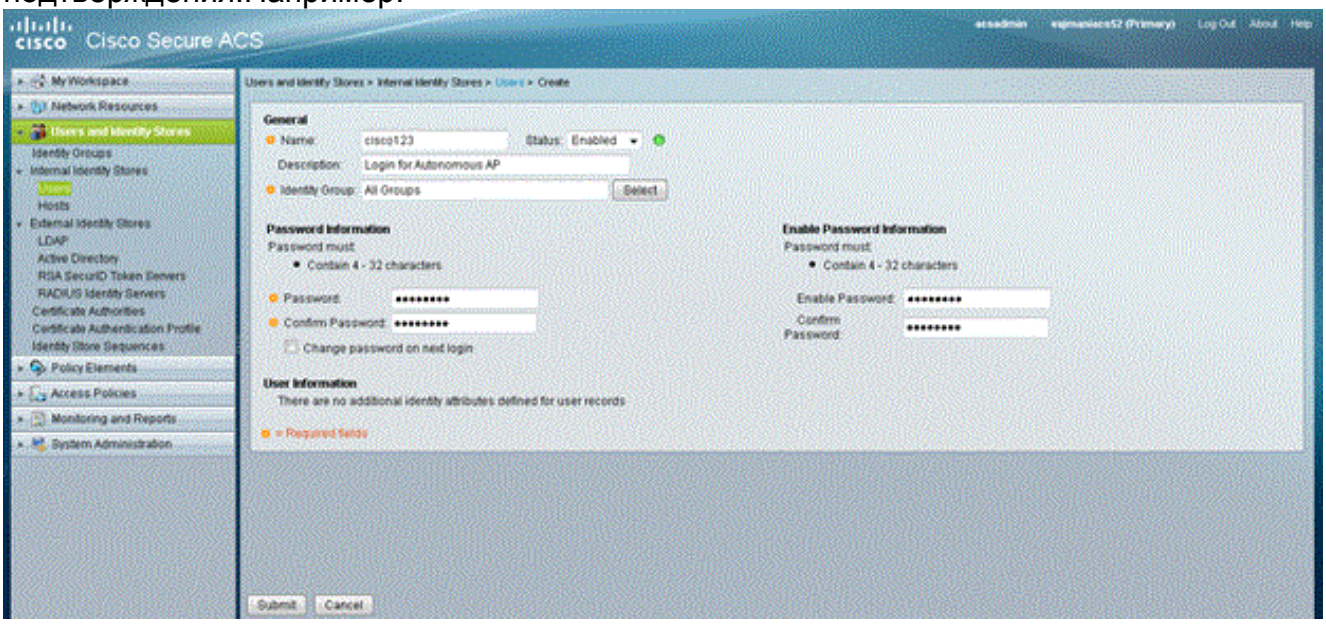
Первый шаг должен добавить AP как клиента AAA в ACS и создать политику TACACS для входа в систему.

1. Выполните эти шаги для добавления AP как клиент AAA:От GUI ACS нажмите **Network Resources**, затем нажмите **Network Devices и AAA Clients**.Под Сетевыми устройствами

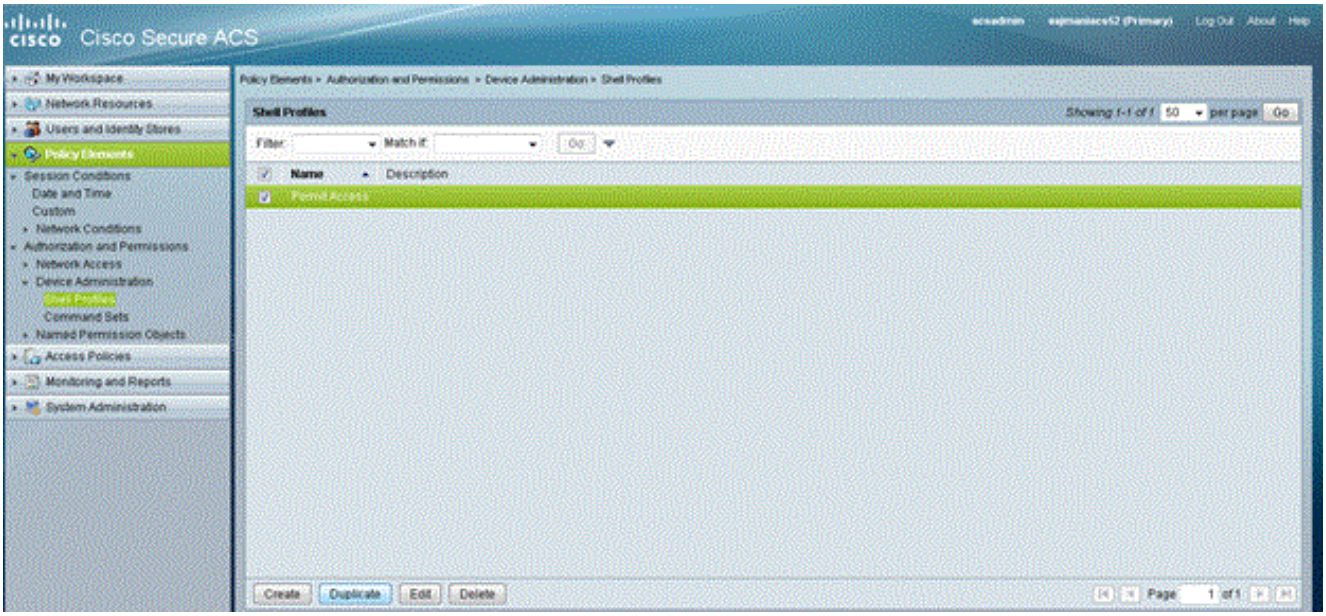
нажмите **Create**.Введите имя хоста AP на **Название** и предоставьте описание о AP.Выберите **Location** и **Device Type**, если определены эти категории.Поскольку только одиночный AP настраивается, нажмите **Single IP Address**. Можно добавить диапазон IP-адресов для множественных AP путем нажатия **IP Range.** Затем введите IP-адрес AP.Под **Параметрами проверки подлинности** проверьте **TACACS +** коробка и введите **Общий секретный ключ**.Например:



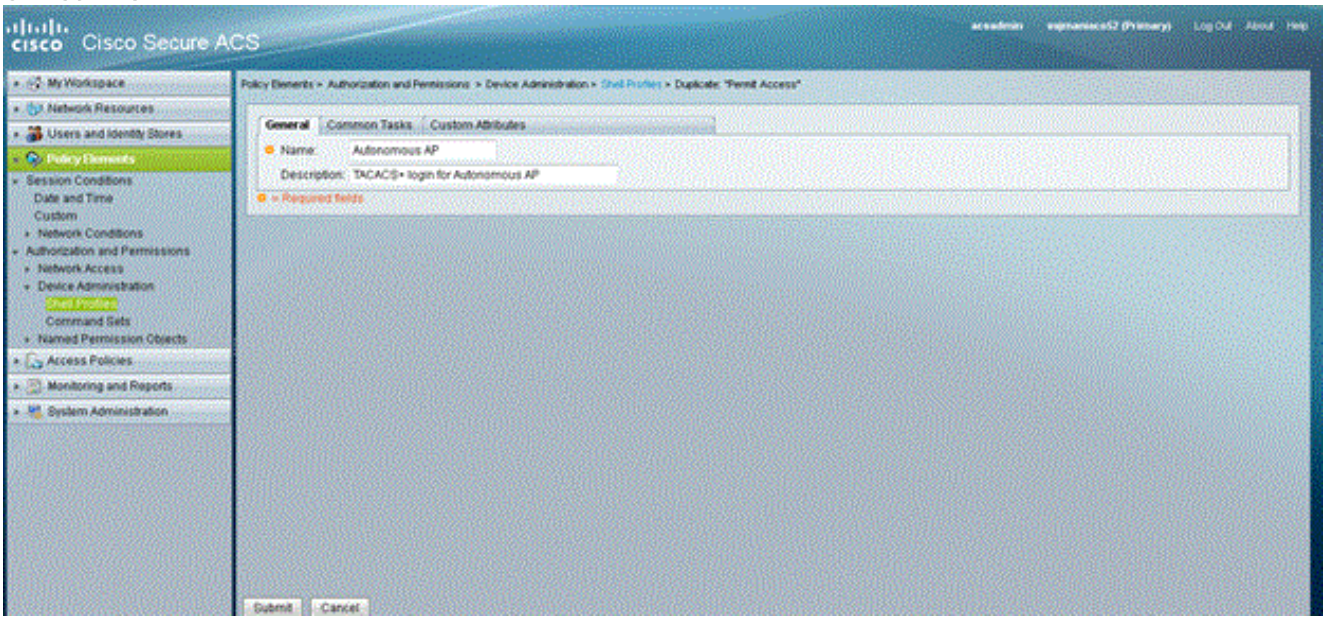
2. Следующий шаг должен создать имя пользователя и пароль входа в систему:Нажмите **Users и Identity Stores**, затем нажмите **Users**.**Нажмите кнопку Create.**Дайте имя пользователя под **Названием** и предоставьте описание.Выберите **Identity Group**, если таковые имеются.Введите пароль под текстовым полем **Пароля** и повторно введите под**, Подтверждают Пароль**.Можно модифицировать enable password путем ввода пароля под **Enable Password**. Повторно введите для подтверждения.Например:



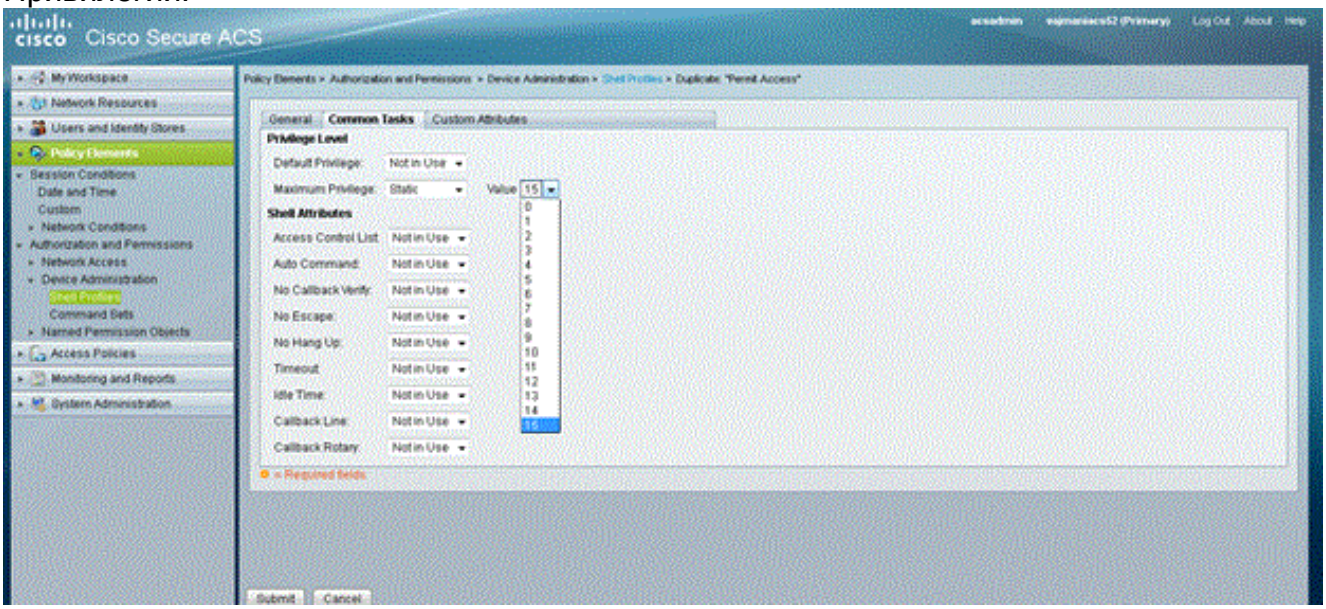
3. Выполните эти шаги для определения уровня привилегий:Нажмите **Policy Elements> Authorizations и Permissions> Device Administration> Shell Profiles**.Установите флажок **Проверки доступа Разрешения** и нажмите **Duplicate**.



Введите **имя** и **описание**.

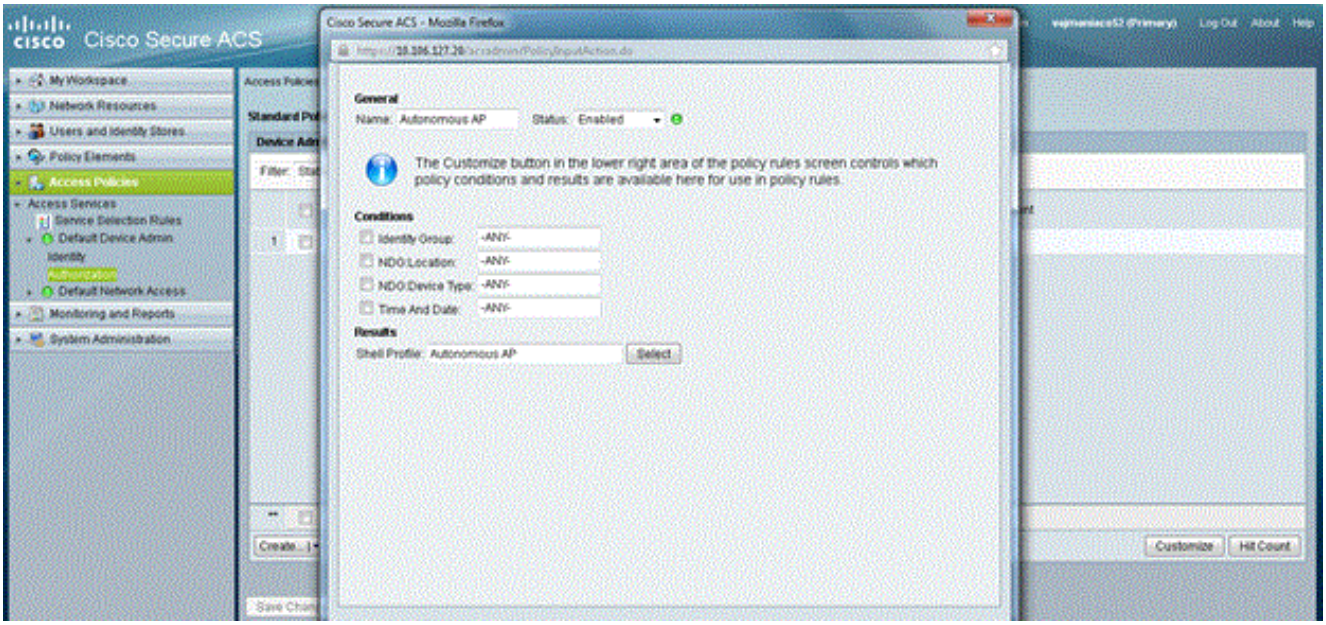


Выберите вкладку Common Tasks и выберите **15** для Максимальной Привилегии.

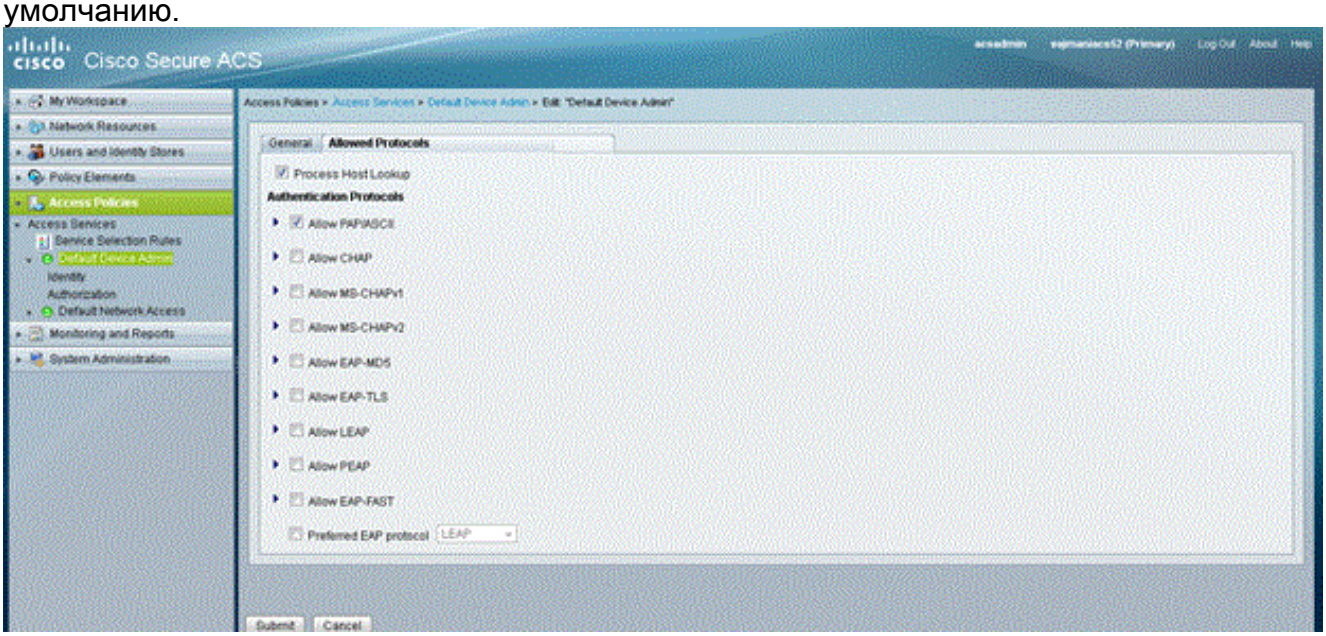


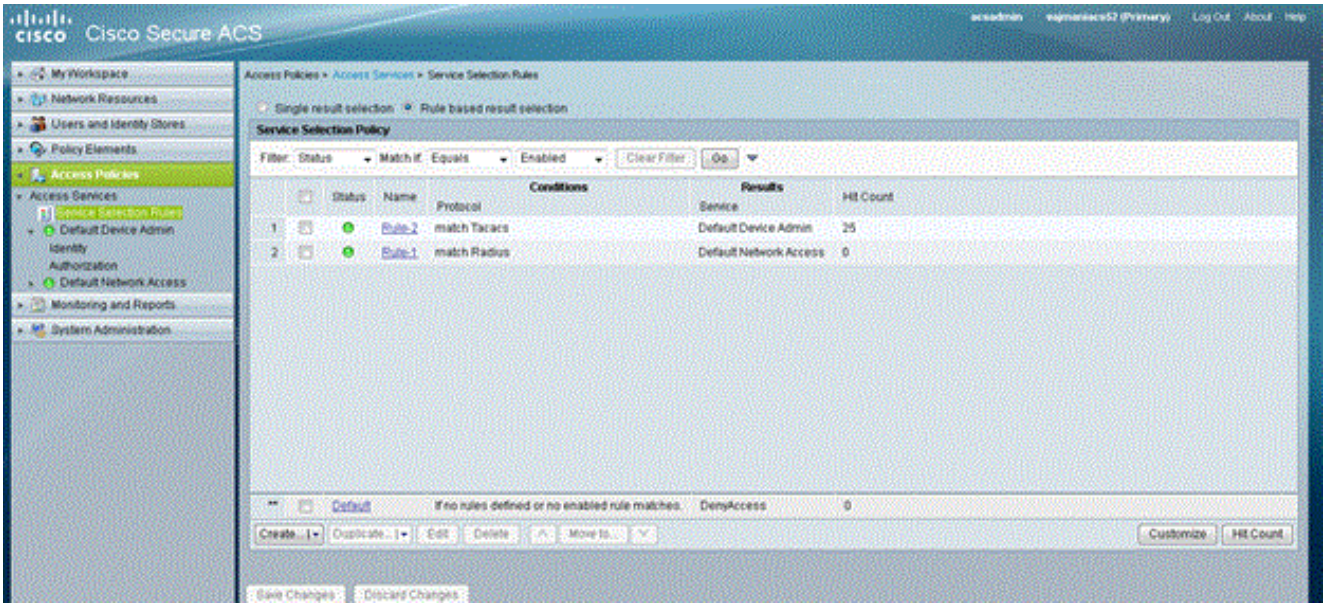
Нажмите кнопку Submit (Отправить).

4. Выполните эти шаги для создания Политики авторизации:Нажмите **Access Policies> Access Services> Default Device Admin> Authorization**.Нажмите **Create** для создания новой Политики авторизации.Новое всплывающее окно, кажется, создает правила для Политики авторизации.Выберите **Identity Group**, **Location** и т.д. для определенного имени пользователя и клиента AAA (AP), если таковые имеются.Нажмите **Select** для Профиля Shell для выбора, профиль создал Автономный AP.



Как только это сделано, нажмите **Save Changes**.Нажмите **Default Device Admin**, затем нажмите **Allowed Protocols**.Проверка **Позволяет PAP/ASCII**, затем нажимает **Submit**.Нажмите **Service Selection Rules**, чтобы удостовериться, что существует правило соответствующий TACACS и указывающий на Администратора устройства по умолчанию.



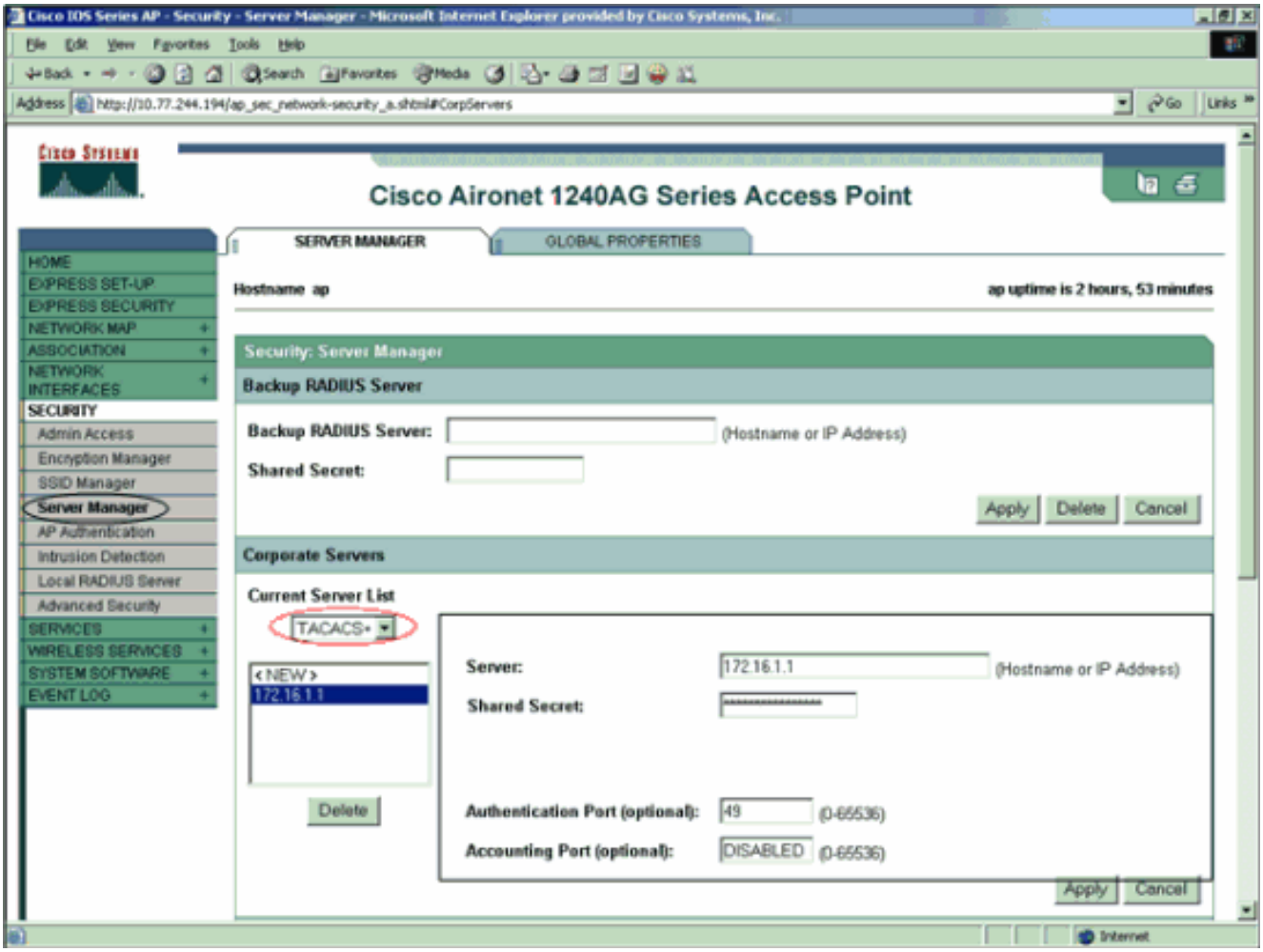


Настройте AP Aironet для TACACS + аутентификация

Можно использовать или CLI или GUI для включения TACACS + функции на AP Aironet. Этот раздел объясняет, как настроить AP для TACACS + login authentication с использованием GUI.

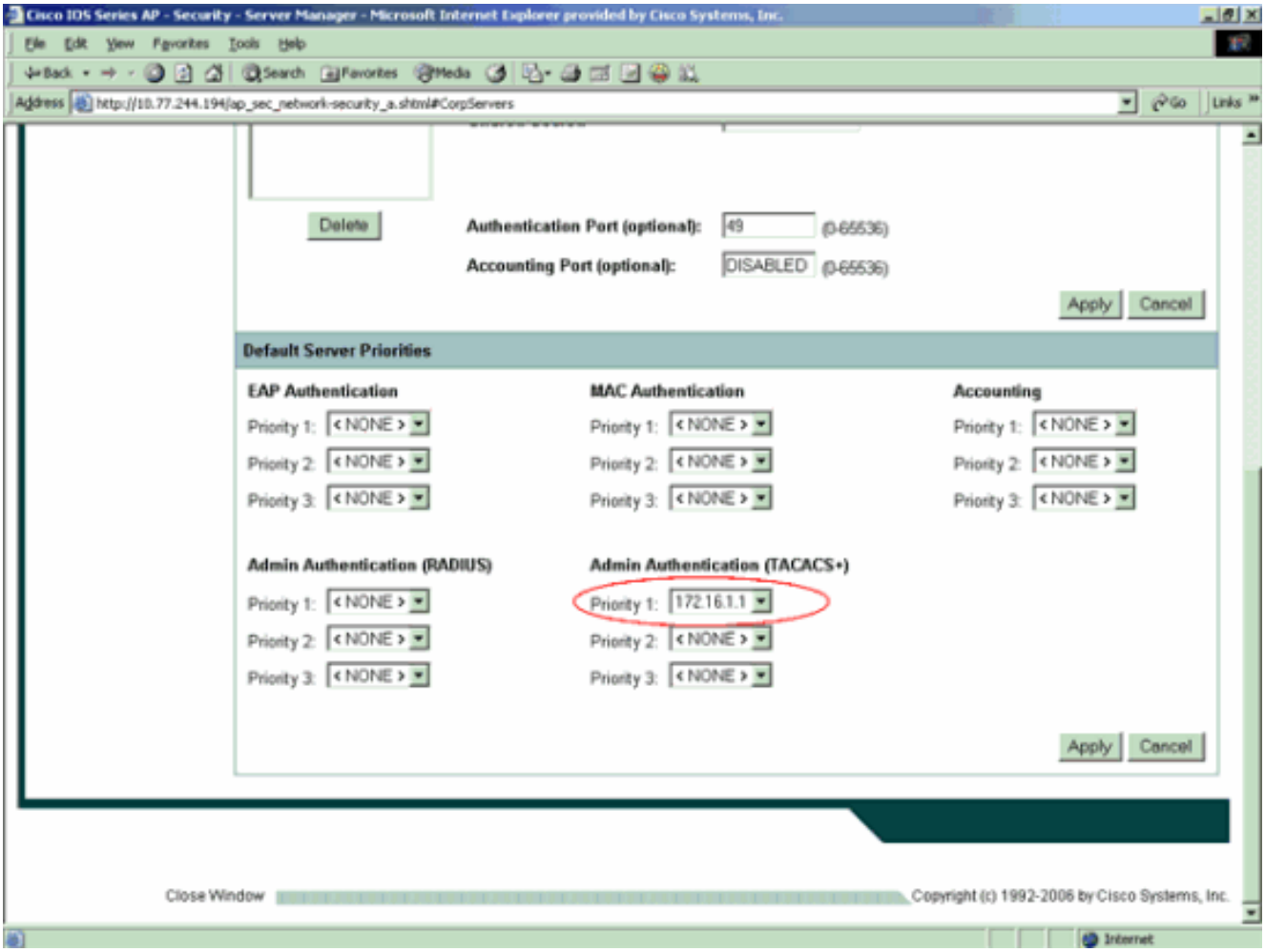
Выполните эти шаги для настройки TACACS + на AP с использованием GUI:

1. Выполните эти шаги для определения TACACS + параметры сервера:От GUI AP выберите **Security> Server Manager**.Безопасность: Окно менеджера сервера появляется.В области Corporate Servers выберите **TACACS +** от раскрывающегося меню Списка Текущего сервера.В этой той же области введите IP-адрес, общий секретный ключ и количество порта аутентификации TACACS + сервер.**Щелкните "Применить".**Например:

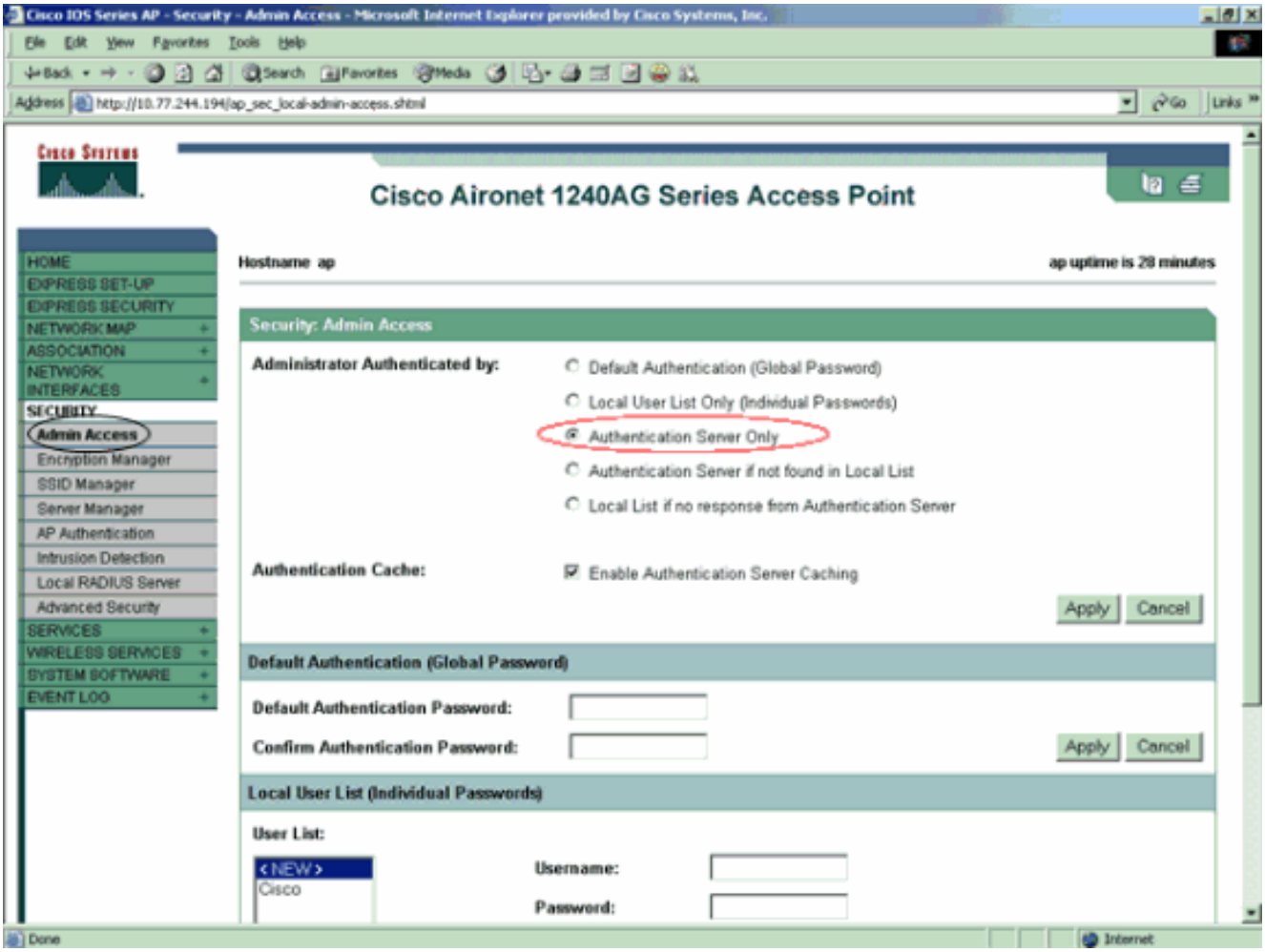


Примечание: По умолчанию TACACS + использует порт TCP 49.**Примечание:** Общий секретный ключ, который вы настраиваете на ACS и AP, должен совпасть.

2. Выберите **Default Server Priorities> Admin Authentication (TACACS +)**, выберите от Приоритета 1 раскрывающееся меню TACACS + IP-адрес сервера, который вы настроили и нажимаете **Apply**.Например:



3. Выберите **Security> Admin Access** и для Администратора, Аутентифицируемого: выберите **Authentication Server Only** и нажмите **Apply**.Этот выбор гарантирует, что пользователи, которые пытаются войти к AP, аутентифицируются сервером проверки подлинности.Например:



Это - конфигурация интерфейса командой строки для примера конфигурации:

Точка доступа
AccessPoint#**show running-config** Current configuration : 2535 bytes ! version 12.3 no service pad service timestamps debug datetime msec service timestamps log datetime msec service password-encryption ! hostname AccessPoint ! ! ip subnet-zero ! ! **aaa new-model** *!--- Enable AAA.* ! ! aaa group server radius rad_eap ! aaa group server radius rad_mac ! aaa group server radius rad_acct ! aaa group server radius rad_admin cache expiry 1 cache authorization profile admin_cache cache authentication profile admin_cache ! **aaa group server tacacs+ tac_admin** *!--- Configure the server group tac_admin.* **server 172.16.1.1** *!--- Add the TACACS+ server 172.16.1.1 to the server group.* **cache expiry 1** *!--- Set the expiration time for the local cache as 24 hours.* **cache authorization profile admin_cache cache authentication profile admin_cache** ! aaa group server radius rad_pmip ! aaa group server radius dummy ! **aaa authentication login default group tac_admin** *!--- Define the AAA login authentication method list to use the TACACS+ server.* aaa authentication login eap_methods group rad_eap aaa authentication login mac_methods local **aaa authorization exec default group tac_admin** *!--- Use TACACS+ for privileged EXEC access authorization !--- if authentication was performed with use of TACACS+.* aaa accounting network acct_methods start-stop group rad_acct aaa cache profile admin_cache all ! aaa session-id common ! ! username Cisco password 7 00271A150754 ! bridge irb ! ! interface Dot11Radio0 no ip address no ip route-cache shutdown speed basic-1.0

```
basic-2.0 basic-5.5 basic-11.0 station-role root bridge-
group 1 bridge-group 1 subscriber-loop-control bridge-
group 1 block-unknown-source no bridge-group 1 source-
learning no bridge-group 1 unicast-flooding bridge-group
1 spanning-disabled ! interface Dot11Radio1 no ip
address no ip route-cache shutdown speed station-role
root bridge-group 1 bridge-group 1 subscriber-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding bridge-group 1 spanning-disabled ! interface
FastEthernet0 no ip address no ip route-cache duplex
auto speed auto bridge-group 1 no bridge-group 1 source-
learning bridge-group 1 spanning-disabled ! interface
BVI1 ip address 172.16.1.30 255.255.0.0 no ip route-
cache ! ip http server ip http authentication aaa !---
Specify the authentication method of HTTP users as AAA.
no ip http secure-server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/ea ip radius source-interface BVI1 ! tacacs-server
host 172.16.1.1 port 49 key 7 13200F13061C082F tacacs-
server directed-request radius-server attribute 32
include-in-access-req format %h radius-server vsa send
accounting ! control-plane ! bridge 1 route ip ! ! !
line con 0 transport preferred all transport output all
line vty 0 4 transport preferred all transport input all
transport output all line vty 5 15 transport preferred
all transport input all transport output all ! end
```

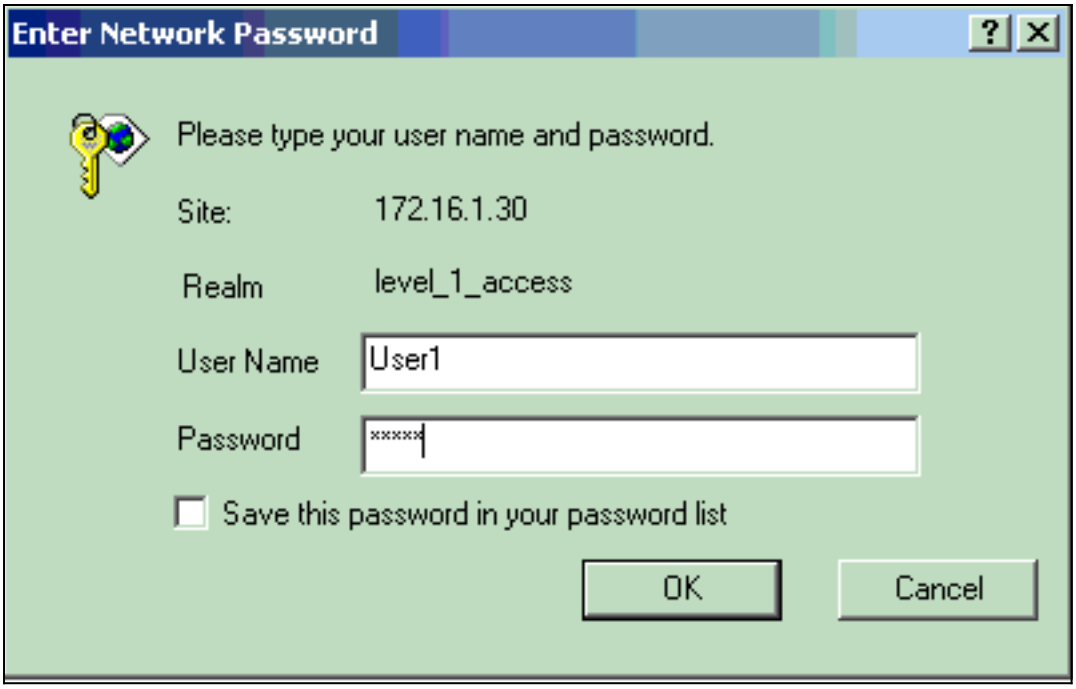
Примечание: У вас должно быть программное обеспечение Cisco IOS версии 12.3 (7) JA или позже для всех команд в этой конфигурации для работы должным образом. Более ранний Cisco IOS Software Release не мог бы иметь все эти команды в наличии.

Проверка

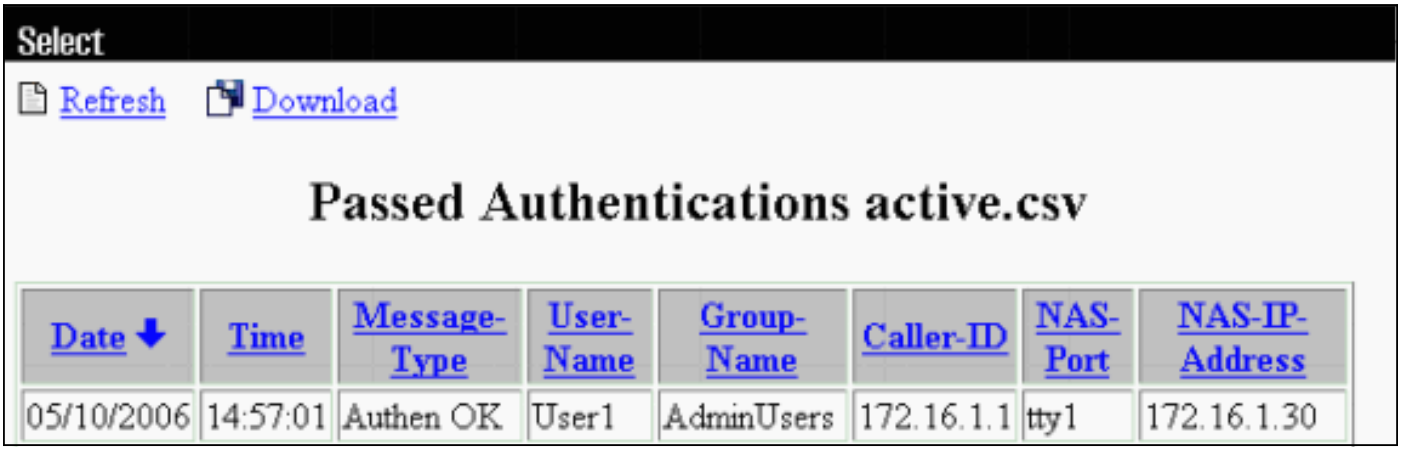
Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Для проверки конфигурации попытайтесь войти к AP с использованием GUI или CLI. Когда вы пытаетесь обратиться к AP, AP побуждает вас для имени пользователя и пароля.



Когда вы предоставляете учетные данные пользователя, AP вперед учетные данные к TACACS + сервер. TACACS + сервер проверяет учетные данные на основе информации, которая доступна в ее базе данных и предоставляет доступ к AP после успешной аутентификации. Можно выбрать **Reports и Activity> Passed Authentication** на ACS и использовать Переданный Опознавательный отчёт для проверки для успешной аутентификации для этого пользователя. Например:



Можно также использовать **команду show tacacs** для проверки корректной конфигурации TACACS + сервер. Например:

```
AccessPoint#show tacacs Tacacs+ Server : 172.16.1.1/49 Socket opens: 348 Socket closes: 348
Socket aborts: 0 Socket errors: 0 Socket Timeouts: 0 Failed Connect Attempts: 0 Total Packets
Sent: 525 Total Packets Recv: 525
```

Проверка для ACS 5.2

Можно проверить, Отказал/Передал попытки для учетных данных входа в систему от ACS 5.2:

1. Нажмите **Monitoring and Reports> Launch Monitoring and Report Viewer**.Новое всплывающее окно открывается Информационной панелью.
2. Нажмите **Authentications-TACACS-Today**. Это показывает, что подробные данные отказали/передали попытки.

Устранение неполадок

Можно использовать эти команды отладки на AP для устранения проблем конфигурации:

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **события debug tacacs** — Эта команда отображает последовательность событий, которые происходят во время Аутентификации TACACS. Вот пример выходных данных этой команды:*Mar 1 00:51:21.113: TPLUS: **Queuing AAA Authentication request 0 for processing** *Mar 1 00:51:21.113: TPLUS: processing authentication start request id 0 *Mar 1 00:51:21.113: TPLUS: **Authentication start packet created for 0(User1)** *Mar 1 00:51:21.114: TPLUS: **Using server 172.16.1.1** *Mar 1 00:51:21.115: TPLUS(00000000)/0/NB_WAIT/C6DC40: Started 5 sec timeout *Mar 1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: socket event 2 *Mar 1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request *Mar 1 00:51:21.116: TPLUS(00000000)/0/READ: socket event 1 *Mar 1 00:51:21.117: TPLUS(00000000)/0/READ: Would block while reading *Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1 *Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16 bytes data) *Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1 *Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 28 bytes response *Mar 1 00:51:21.121: TPLUS(00000000)/0/C6DC40: Processing the reply packet *Mar 1 00:51:21.121: TPLUS: **Received authen response status GET_PASSWORD (8)** *Mar 1 00:51:21.121: TPLUS: Queuing AAA Authentication request 0 for processing *Mar 1 00:51:21.121: TPLUS: processing authentication continue request id 0 *Mar 1 00:51:21.122: TPLUS: Authentication continue packet generated for 0 *Mar 1 00:51:21.122: TPLUS(00000000)/0/WRITE/C6DC40: Started 5 sec timeout *Mar 1 00:51:21.122: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request *Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1 *Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6 bytes data) *Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1 *Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 18 bytes response *Mar 1 00:51:21.179: TPLUS(00000000)/0/C6DC40: **Processing the reply packet** *Mar 1 00:51:21.179: TPLUS: **Received authen response status PASS (2)**
- **debug ip http authentication — используется для устранения неполадок с HTTP-аутентификацией.** Команда отображает метод аутентификации, которого маршрутизатор делал попытку и опознавательно-специфичные сообщения о статусе.
- **debug aaa authentication** — Эта команда отображает информацию на TACACS AAA + аутентификация.

Если пользователь вводит имя пользователя, которое не существует на TACACS + сервер, опознавательные сбои. Вот выходные данные **команды debug tacacs authentication** для ошибки проверки подлинности:

*Mar 1 00:07:26.624: TPLUS:**Queuing AAA Authentication request 0 for processing** *Mar 1 00:07:26.624: TPLUS: processing authentication start request id 0 *Mar 1 00:07:26.624: TPLUS: Authentication start packet created for 0(User3) *Mar 1 00:07:26.624: TPLUS: **Using server 172.16.1.1** *Mar 1 00:07:26.625: TPLUS(00000000)/0/NB_WAIT/A88784: Started 5 sec timeout *Mar 1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: socket event 2 *Mar 1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request *Mar 1 00:07:26.627: TPLUS(00000000)/0/READ: socket event 1 *Mar 1 00:07:26.627: TPLUS(00000000)/0/READ: Would block while reading *Mar 1 00:07:26.631: TPLUS(00000000)/0/READ: socket event 1 *Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16 bytes data) *Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: socket event 1 *Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 28 bytes response *Mar 1 00:07:26.632: TPLUS(00000000)/0/A88784: Processing the reply packet *Mar 1 00:07:26.632: TPLUS: **Received authen response status GET_PASSWORD (8)** *Mar 1 00:07:26.632: TPLUS: Queuing AAA Authentication request 0 for processing *Mar 1 00:07:26.633: TPLUS: processing authentication continue request id 0 *Mar 1 00:07:26.633: TPLUS: Authentication continue packet generated for 0 *Mar 1 00:07:26.634: TPLUS(00000000)/0/WRITE/A88784: Started 5 sec timeout *Mar 1 00:07:26.634: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request *Mar 1 00:07:26.688:

```
TPLUS(00000000)/0/READ: socket event 1 *Mar 1 00:07:26.688: TPLUS(00000000)/0/READ: read entire
12 header bytes (expect 6 bytes data) *Mar 1 00:07:26.689: TPLUS(00000000)/0/READ: socket event
1 *Mar 1 00:07:26.689: TPLUS(00000000)/0/READ: read entire 18 bytes response *Mar 1
00:07:26.689: TPLUS(00000000)/0/A88784: Processing the reply packet *Mar 1 00:07:26.689: TPLUS:
Received authen response status FAIL (3)
```

Можно выбрать **Reports и Activity> Failed Authentication** для наблюдения неудачной попытки аутентификации на ACS. Например:

Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	Authen-Failure-Code	Author-Failure-Code	Author-Data	NAS-Port
05/17/2006	19:40:14	Authen failed	User3	..	..	CS user unknown	..	..	..

При использовании Cisco IOS Software Release на AP, который является ранее, чем программное обеспечение Cisco IOS версии 12.3 (7) JA, можно поразить дефект каждый раз, когда вы пытаетесь войти к AP с использованием HTTP. Идентификатор ошибки Cisco является CSCeb52431 (только зарегистрированные клиенты).

Реализация HTTP/AAA программного обеспечения Cisco IOS требует независимой аутентификации каждого отдельного соединения HTTP. Беспроводной GUI программного обеспечения Cisco IOS включает ссылку многих десятков отдельных файлов в одиночной веб-странице (например, Javascript и GIF). Таким образом, при загрузке одиночной страницы в беспроводном GUI программного обеспечения Cisco IOS десятки и десятки отдельной аутентификации/запросов авторизации могут поразить AAA-сервер.

Для проверки подлинности HTTP используйте RADIUS или локальную проверку подлинности. Сервер RADIUS все еще подвергнут запросам несколько серверов проверок подлинности. Но RADIUS является более масштабируемым, чем TACACS +, и таким образом, это, вероятно, предоставит менее - неблагоприятное влияние на производительность.

Если необходимо использовать TACACS +, и вы имеете ACS Cisco, используете ключевое слово **single-connection** с **командой tacacs-server**. Использование этого ключевого слова с командой экономит ACS большая часть настройки/освобождения служебной информации TCP - подключения и, вероятно, уменьшит загрузку на сервере до некоторой степени.

Для Cisco IOS Software Release 12.3 (7) JA и позже AP, программное обеспечение включает исправление. Остаток от этого раздела описывает исправление.

Используйте функцию кэша аутентификации AAA (проверка подлинности, авторизация и учет) для кэширования информации, которую возвращает TACACS + сервер. Опознавательная функция кэша и профиля позволяет AP кэшировать аутентификацию/отклики при авторизации для пользователя так, чтобы последующая аутентификация / запросы авторизации не должна была быть передана AAA-серверу. Для активации этой опции с CLI используйте эти команды:

```
cache expiry cache authorization profile cache authentication profile aaa cache profile
```

Для получения дополнительной информации об этой функции и командах, обратитесь к *Настройке Опознавательный* раздел *Кэша и Профиля* Администрирования точки доступа.

Для активации этой опции на GUI выберите **Security> Admin Access** и проверьте флажок **Enable Authentication Server Caching**. Поскольку этот документ использует программное

обеспечение Cisco IOS версии 12.3 (7) JA, документ использует исправление, поскольку конфигурации иллюстрируют.

Дополнительные сведения

- Настройка серверов RADIUS и TACACS+
- Уведомление о дефекте: Точка доступа IOS бомбардирует TACACS + сервер с запросами
- Аутентификация EAP с помощью сервера RADIUS
- Поддержка беспроводного продукта
- Cisco Systems – техническая поддержка и документация